AFFIDAVIT OF TASK FORCE OFFICER MICHAEL SULLIVAN IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Michael Sullivan, a Task Force Officer, with the Federal Bureau of Investigation ("FBI"), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am employed as a Sergeant Detective with the City of Boston (Massachusetts) Police Department. I am also a sworn Special Deputy United States Marshal. I have been employed by the Boston Police Department since October 2005 and am currently assigned as a Task Force Officer to the FBI Boston Division, Child Exploitation and Human Trafficking Task Force. While employed by the Boston Police Department, I have investigated state and federal criminal violations related to, among other things, the on-line sexual exploitation of children. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

2. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in Attachment A of this Affidavit, including the entire property located at 284 S. Christopher Avenue, Tiverton, Rhode Island (the "SUBJECT PREMISES"), including the content of electronic storage devices located therein, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A (possession and receipt of child pornography), which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements in this affidavit are based in part on information provided by FBI Special Agents and analysts; information gathered from the service of administrative subpoenas;

the results of physical and electronic surveillance conducted by law enforcement agents; and my experience, training, and background as a Special Agent with the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A are presently located at the SUBJECT PREMISES.

STATEMENT OF PROBABLE CAUSE

Background Regarding Freenet

4. The instant investigation involves a user of "Freenet" — which is an Internet-based peer-to-peer (P2P) network that allows users to anonymously share files, chat on message boards, and access websites within the network. Law enforcement agents have been investigating child pornography trafficking by Freenet users since at least 2011.

5. In order to access Freenet, a user must first download the Freenet software, which is free and publicly available. The Freenet "source code" — i.e., the computer programming code that facilitates Freenet's operation – is also publicly available. In other words, Freenet is "open source" software that may be examined and analyzed by anyone with the pertinent expertise or knowledge.

6. Anyone running the Freenet software may join and access the Freenet network. Each computer running Freenet connects directly to other computers running Freenet, which are

called its "peers."[1] When installing Freenet, each user agrees to provide to the network a portion of the storage space on the user's computer hard drive, so that files uploaded by Freenet users can be distributed and stored across the network. Freenet users can upload files into the Freenet network and download files from the Freenet network. After a user installs Freenet on the user's computer, the software creates a default "download" folder. If a user successfully downloads a particular file from Freenet, Freenet may save the content of that file to the "download" folder. A user may change this default setting and direct the content to be downloaded elsewhere.

7. When a user uploads a file into Freenet, the software breaks the file into pieces (called "blocks") and encrypts each piece. The encrypted pieces of the file are then distributed randomly and stored throughout the Freenet network of peers.[2] The software also creates an index piece that contains a list of all of the pieces of the file and a unique key – a series of letters, numbers and special characters – that is used to download the file.[3]

8. In order to download a file on Freenet, a user must have the key for the file. There are a number of ways that a Freenet user can download a file using a key. Some examples include: (1) the "download" box on Freenet's "file sharing" page; (2) the "download" box on the message board associated with Freenet or other Freenet add-on programs; and (3) directly through the user's web browser while the user is connected to the Freenet network.

9. When a user attempts to download a file via Freenet, Freenet downloads the piece

[1] The number of peers is determined by the user's settings and is based on the quality and speed of the user's Internet connection.

[2] Because the pieces of files are encrypted, a Freenet user is unable to access the content of pieces that are stored on the user's computer hard drive, which are not in a readable format.

[3] An example key is: CHK@0R6h6o8a~JbOGg8GmxGauRyqJPSwcHGmxGauLznw8Fey B0go,08agxRpNx~wc~rmZRfWQaSed3HTeKKkXAwvDRF2LUaU,AAMC--8/lolitaz49.avi.

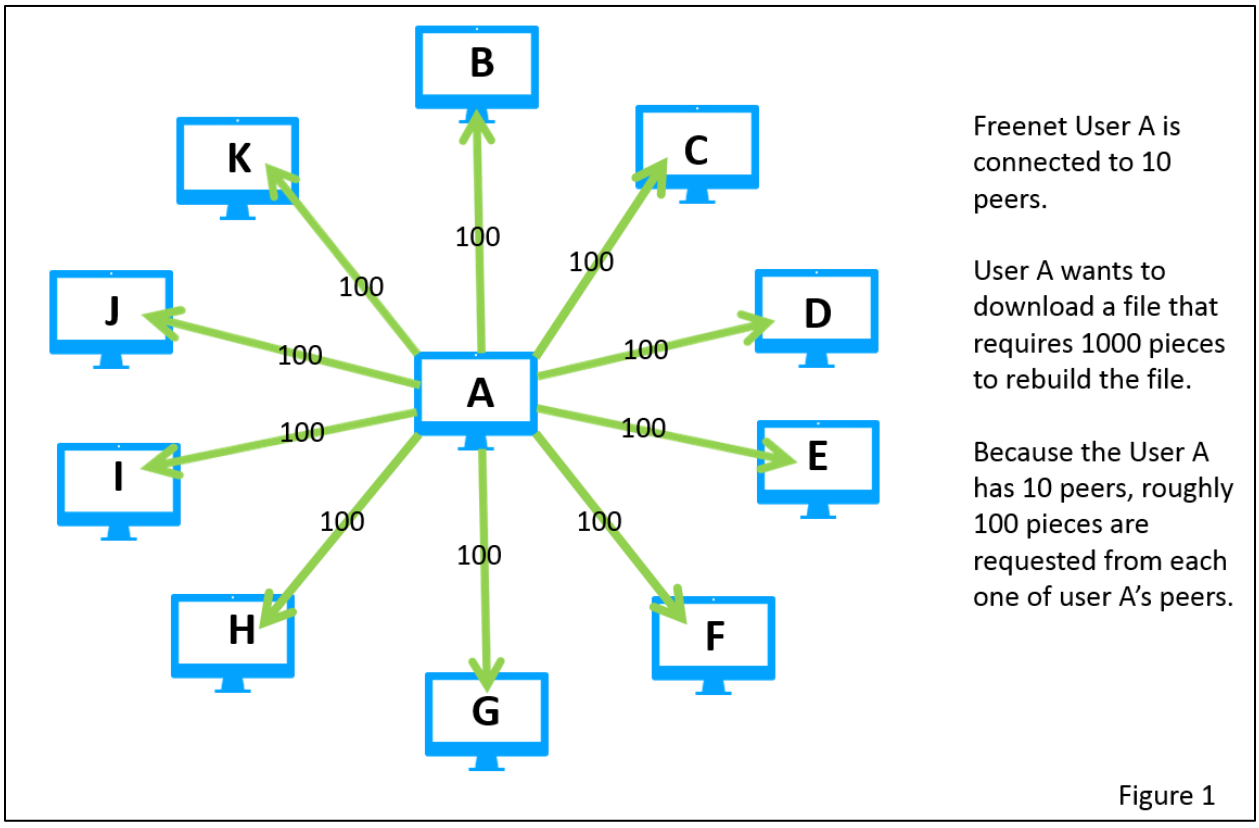

Figure 1

If Peer "B" receives User A's request for 100 pieces of the file, but does not have any of those pieces in its storage, Peer B forwards on the request for those pieces to Peer B's peers. If Peer B has 10 peers of its own, roughly 10 pieces are requested from each one of Peer B's peers. See Figure 2.

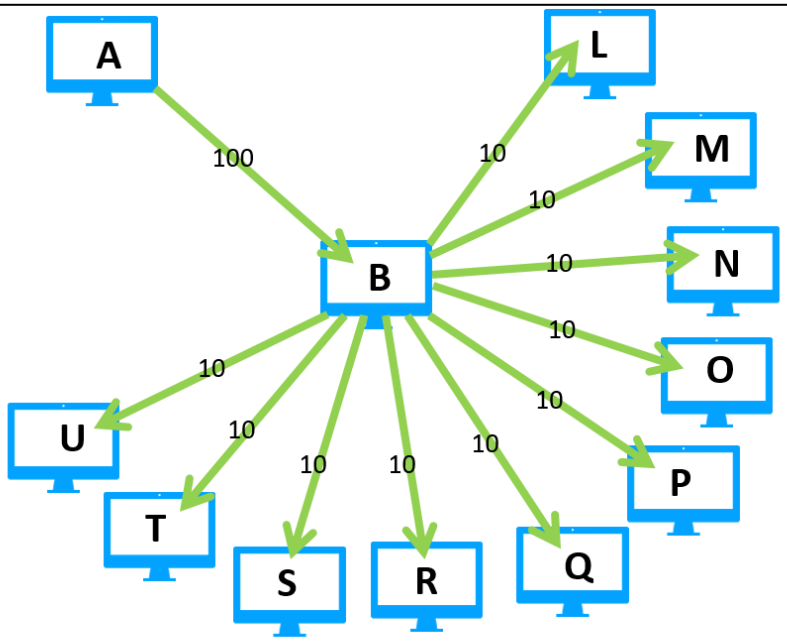

Figure 2

As noted below, this design can help law enforcement distinguish between a Freenet user that is the original requestor of a file, and one that is merely forwarding the request of another user.

10. To prevent requests for pieces from going on indefinitely, Freenet is configured to only allow a request for a piece of a file to be forwarded to another peer a limited number of times (the default maximum is 18). If a request reaches that limit without finding the requested piece, a signal is returned to the user's computer and the request is sent to another of the user's peers. The remaining number of times a request for a piece may be forwarded is included within the request for that piece.

11. Freenet attempts to hide which computer uploaded a file into or downloaded a file from the network by making it difficult to differentiate whether a request for a piece that comes in from a peer originated with that peer (i.e., the peer was the "original requestor" of the file), or whether that peer was simply forwarding a different peer's request. Freenet attempts to hide the

identity of the original requestor by randomizing the initial number of times a request can be forwarded from one peer to another to be either 17 or 18. Without this randomization, any time a user received a request for a piece of a file that could be forwarded 18 times, the user would know that its peer was the original requestor of the file. This design allows investigators using Freenet to focus investigative efforts on peer computers that request pieces of files of interest that may be forwarded 17 or 18 times, in order to determine whether the peer was the original requestor of the file.

12. Freenet has two operational modes, "Darknet" and "Opennet." On the Darknet mode, a computer connects only to peers whom the user has specifically selected. On the Opennet mode, a computer may connect to peers unknown to the user. A Freenet user may choose which mode to use. The mode relevant to this investigation involves a user who chose to use the Opennet operational mode.

13. Freenet warns its users in multiple ways that it does not guarantee anonymity: when Freenet software is initially installed; within the log file each time Freenet is started; and via Freenet's publicly accessible website. Freenet software also does not mask a computer's IP address — the IP addresses of each Freenet user's peers are observable to the user. For example, if a user is connected to 10 peers on Freenet, all 10 of those peers' IP addresses will be observable to the user. The fact that Freenet does not mask IP addresses is explained on its publicly accessible website. Freenet also acknowledges on its publicly accessible website that, for users who use the Opennet mode, it can be statistically shown that a particular user more likely than not requested a file (as opposed to having merely forwarded the request of another peer) based on factors including the proportion of the pieces of a file requested by a user and the number of nearby peers.

Child Pornography Images/Videos on "Freenet"

14. Freenet can be used to advertise and distribute images and videos of child pornography. Unlike other file sharing systems, Freenet does not provide a search function for its users whereby users would insert search terms to locate files. Therefore, a user who wishes to locate and download child pornography from Freenet must identify the key associated with a particular child pornography file and then use that key to download the file.

15. Freenet users can identify those keys in a number of ways. For example, "message boards" exist on Freenet that allow users to post textual messages and engage in online discussions involving the sexual exploitation of minors. Law enforcement agents have observed message boards labeled: "pthc," "boy porn," "hussy," "pedomom," "kidfetish," "toddler_cp," "hurtcore," and "tor-childporn." Typical posts to those message boards contain text, keys of child pornography files that can be downloaded through Freenet, and in some cases descriptions of the image or video file associated with those keys.

16. Freenet users can also obtain keys of child pornography images or videos from websites that operate within Freenet called "Freesites." Freesites can only be accessed through Freenet. Some of those sites contain images of child pornography the user can view along with keys of child pornography files. It is also possible that Freenet users may obtain keys related to child pornography images or videos directly from other Freenet users.

Investigation into the Trafficking of Child Pornography on Freenet

17. Since approximately 2011, law enforcement has been investigating the trafficking of child pornography on Freenet. A modified version of the Freenet software is available to sworn law enforcement officers to assist in conducting Freenet investigations. I have been trained on the

operation of the modified law enforcement version of Freenet. This law enforcement version is nearly identical to Freenet, except that it allows a computer operated by a law enforcement officer to automatically log information about requests for pieces of files received directly from its peers. The types of information logged by a law enforcement computer are available to all standard Freenet users as part of Freenet's normal operation. This information includes but is not limited to: the IP addresses of the user's peers; the number of peers those peers report to have; a unique identifier assigned by the software (referred to as the computer's Freenet "location"); the remaining number of times a request for a piece of a file may be forwarded; the date/time of requests received from a peer; and the digital hash value of a requested piece.

18. Law enforcement computers do not target specific peers on Freenet nor do law enforcement computers solicit requests from any peers. The Freenet information collected by law enforcement computers is logged and provided to other Freenet-trained law enforcement personnel in order to further investigations into Freenet users believed to be downloading child pornography files through Freenet.

19. Law enforcement officers collect keys associated with suspected child pornography files that are being publicly shared and advertised on Freenet. Law enforcement only investigates Freenet users who request pieces of files associated with such keys collected by law enforcement. The keys collected by law enforcement have been obtained via publicly accessible sites, such as Freenet message boards and Freesites, as well as during the course of prior investigations into child pornography trafficking on Freenet. This investigation pertains to child pornography files with known keys, the content of which are further described below. Those files are referenced as "files of interest."

20. By viewing the documented activity of a peer that sends a request to a law enforcement computer, it is possible to determine whether it is significantly more probable than not that the peer is the original requestor of a file of interest. Only those requests that were intended for law enforcement computers as recipients, that may be forwarded 17 or 18 times, and are associated with a file of interest are analyzed. A mathematical formula is then applied to determine the probability of whether the number of requests received for pieces of a file is significantly more than one would expect if the peer were merely forwarding the request of another computer.

21. I have reviewed a peer-reviewed, publicly-available academic paper describing the methodology of that mathematical formula. In basic terms, the methodology relies on two primary facts about the Freenet software: first, the original requestor divides up its requests for pieces of a file among its peers, sending a roughly equal fraction of the requests to each peer; second, if a peer does not have the requested pieces, the peer takes the fraction of requests for pieces of a particular file and divides them up again among its own peers. See Figures 1 and 2, above. Because a peer that is merely routing another peer's request would ask its peers for a significantly smaller portion of the pieces of a file than an original requester, it is possible for the recipient of requests to determine whether a request is significantly more likely than not from an original requestor. The academic paper's detailed evaluation finds that a formal mathematical formula based on this reasoning is highly accurate (specifically, it has a high true positive rate and a low false positive rate).[4] Based upon my training and experience and consultation with others in the field, I believe this to be a reliable method to determine whether it is significantly more probable than not that that a given Freenet computer is the original requestor of a file of interest.

[4] I will make that academic paper available to the court upon request.

22. I am also aware through my training and consultation with others in the field that, prior to the initiation of this particular operation, dozens of searches of digital devices have been conducted by law enforcement officers (either through court-authorization or consent) related to targets whose IP addresses were identified based upon analysis of information from Freenet law enforcement computers, pursuant to which evidence of child pornography possession and/or trafficking was located.

Requests Targeted in the Instant Investigation

23. I have reviewed information obtained and logged by law enforcement Freenet computers related to IP address 98.185.180.207. Such information shows that a Freenet user with IP address 98.185.180.207 requested pieces of the child pornography files described below from a law enforcement Freenet computer. With respect to each file – considering the number of requested file pieces, the total number of file pieces required to assemble the file, and the number of peers the user had – the number of requests for file pieces is significantly more than one would expect to see if the user of IP address 98.185.180.207 were merely routing the request of another user. Accordingly – based on my review of those records, the application of the methodology described above, my understanding of Freenet, my training and experience, and the fact that the same user requested pieces of multiple child pornography files – I believe that the user of IP address 98.185.180.207 was the original requestor of each of the described files.

24. On Sunday, June 13, 2021, between 4:09 PM UTC and Monday, June 14, 2021 at 3:51 PM UTC, a computer running Freenet software, with an IP address of 98.185.180.207, with an average of 28.6 peers, requested from a law enforcement computer 287 out of 8,320 total pieces needed to assemble a file with a SHA1 digital hash value of

3QYYBTBGLPXWUCNLF2MXPYZGITJYSKYY.[5] A law enforcement officer with the FBI has downloaded the exact same file with the above referenced SHA1 hash value from Freenet, and provided that file to me for review. This file is a video which is approximately 23 minutes and 15 seconds long. In the video, a female child who appears to be approximately about 10 to 12 years old is using her hands to masturbate a prepubescent boy's penis. The female child then inserts the penis into her mouth. The female then lays on her back while the boy uses his tongue on the female's vagina. The male is later observed masturbating his penis and touching the female's vagina. The male then places his penis into the female's vagina.[6]

25. On Sunday, June 13, 2021 between 4:24 PM UTC and Monday, June 14, 2021 at

[5] "SHA1" stands for "secure hash algorithm – 1" and refers to a particular type of cryptographic hash value. In simple terms, a hash value is an alphanumeric value that uniquely identifies data.

[6] I am aware that the "preferred practice" in the First Circuit is that a magistrate judge view images that agents believe constitute child pornography by virtue of their lascivious exhibition of a child's genitals. *United States v. Brunette*, 256 F.3d 14, 17-19 (1st Cir. 2001) (affiant's "legal conclusion parroting the statutory definition […] absent any descriptive support and without an independent review of the images" insufficient basis for determination of probable cause). Here, however, the descriptions offered "convey to the magistrate more than [my] mere opinion that the images constitute child pornography." *United States v. Burdulis*, 753 F.3d 255, 261 (1st Cir. 2014) (distinguishing *Brunette*). The children described herein are approximately 8-15 years old – in all events, younger than eighteen. Furthermore, the descriptions of the files here are sufficiently specific as to the age and appearance of the alleged children as well as the nature of the sexual conduct pictured in each file, such that the Court need not view the files to find that they depict child pornography. *See United States v. Syphers*, 426 F.3d 461, 467 (1st Cir. 2005) ("The best practice for an applicant seeking a warrant based on images of alleged child pornography is for an applicant to append the images *or provide a sufficiently specific description of the images* to enable the magistrate judge to determine independently whether they probably depict real children.") (emphasis added); *see also United States v. LaFortune*, 520 F.3d 50, 56 (1st Cir. 2008) (similarly emphasizing *Syphers* court's use of "or" in describing the *Brunette* "best practice"). Where I have included such nonconclusory, sufficiently specific descriptions, this Court need not view the imagery to find that they depict child pornography. Nonetheless, the described imagery is available for review at the Court's request.

9:26 AM UTC, a computer running Freenet software, with an IP address of 98.185.180.207, with an average of 28.7 peers, requested from a law enforcement computer 98 out of 2,815 total pieces needed to assemble a file with a SHA1 digital hash value of OAHUNXLCY6FT27OMD34JTDAUTWHCT7IL. A law enforcement officer with the FBI has downloaded the exact same file with the above referenced SHA1 hash value from Freenet, and provided that file to me for review. This file is a video which is approximately 14 minutes and 56 seconds long. In the video, a fully dressed female who appears to be approximately 8-10 years old, is observed dancing on what appears to be a video chat. During this video, the child lifts up her shirt exposing her stomach and pulls down her pants exposing her buttocks. The child takes off her pants as she continues dancing with her top on and underwear on. As the video continues the female removes her top exposing her bare chest. During brief moments, the child exposes her pubic area to the camera. The child eventually presents fully naked and while continuing to dance exposes and grabs her buttocks with her hand while at times exposing her pubic area. The female faces the camera with her legs spread apart and the camera is focused on the child's abdomen down to her knees.

26. On Sunday, June 6, 2021 between 10:29 AM UTC and Sunday, June 6, 2021 at 1:02 PM UTC, a computer running Freenet software with an IP address of 98.185.180.207, with an average of 24.2 peers, requested from a law enforcement computer 83 out of 1,440 pieces needed to assemble a file with a SHA1 digital hash value of G7JFGMCE3N5TNOZW3G7NJVIIYSQI2Y3P. A law enforcement officer with the FBI has downloaded the exact same file with the above referenced SHA1 hash value from Freenet, and provided that file to me for review. This file is a video which is approximately 13 minutes and 6

seconds long. The video presents a female, about 10 to 12 years old, laying naked on her back. The video continues as it focuses in on the female's vagina. A white string is observed protruding from her vagina. The female uses her hands to pull open her vagina and is observed manipulating the string. The female then pulls this string out and it appears to be a tampon. The female then places this object into her mouth. The female inserts her finger into her vagina and then into her mouth.

27. The fact that a Freenet user requested pieces associated with a particular file on Freenet indicates that the user attempted to download the file's contents from Freenet. It does not indicate whether or not the user successfully retrieved all of the necessary pieces to successfully download the file.

28. The keys for each of these files were obtained by law enforcement agents at some point between 2011 and the present date either from a Freenet message board or Freesite that contained information related to the sexual exploitation of children, or from a previous investigation. I am not aware of how, or from where, this particular Freenet user obtained a key in order to attempt to retrieve the files of interest described.

Identification of the SUBJECT PREMISES

29. Using publicly available search tools, law enforcement determined that IP address 98.185.180.207 is controlled by Internet Service Provider ("ISP") Cox Communications, Inc.

30. On or about August 13, 2021, an FBI administrative subpoena/summons was served on Cox Communications, Inc. for subscriber information relating to the use of the IP address on the following dates and times IP 98.185.180.207 and Port 10611 on June 14, 2021 at 05:44:05 UTC; IP 98.185.180.207 and Port 10611 on June 14, 2021 at 15:51:45 UTC; IP

98.185.180.207 and Port 10611 on June 13, 2021 at 18:04:55 UTC; IP 98.185.180.207 and Port 10611 on June 14, 2021 at 09:26:41 UTC; IP 98.185.180.207 and Port 6939 on June 06, 2021 at 10:29:28 UTC; IP 98.185.180.207 and Port 6939 on June 06, 2021 at 13:02:49 UTC The subscriber information returned on or about September 21, 2021 included, among other information, the following:

IP ADDRESS:	98.185.180.207
Start Time:	2021-03-12 05:44:14 UTC
Stop Time:	2021-09-22 09:44:03 UTC
Customer Name:	Dave Burke
Account Address:	284 S Christopher Ave, Tiverton, RI, 02878-3866

31. Information held by the Registry of Motor Vehicles, which I reviewed on or about September 28, 2021, indicates that an individual named David Burke with a date of birth of 10/29/1958 resides at the SUBJECT PREMISES. Information Northeast Revaluation Group LLC identified David Burke as the owner of 284 South Christopher Avenue in Tiverton, RI.

32. During surveillance of the SUBJECT PREMISES, law enforcement personnel associated with this investigation have not observed any vehicles in the driveway. However, law enforcement personnel observed a large garage.

33. A search of a commercially-available database that aggregates public and private records held by various third parties was conducted for David Burke with a date of birth 10/29/1958. These public records indicated that David Burke's current address is the SUBJECT PREMISES, and was his only listed address during the timeframe of the Freenet downloads.

Characteristics Common to Consumers of Child Pornography

34. Based on my previous training and experience related to investigations involving child pornography and the sexual abuse of children, I have learned that individuals who create,

possess, receive, distribute, or access with intent to view child pornography (collectively, "consumers" of child pornography) have a sexual interest in children and in images of children. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to such consumers of child pornography, as outlined in the following paragraphs.

35. The majority of consumers of child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

36. Consumers of child pornography may collect sexually explicit materials, which may consist of hard copy and digital images and videos for their own sexual gratification. These individuals often also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found on computers and digital storage devices that also contain child pornography, or that are used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.

37. Many consumers of child pornography maintain their sexually explicit materials for several years and may go to great lengths to conceal and protect from discovery, theft, and

damage their collections of illicit materials.[7] They regularly maintain their collections in the privacy and security of their homes, inside their cars, on their person, or in cloud-based online storage. Depending on their technical expertise, access to child pornography on seemingly "safe" networks like Tor, or struggle with addiction to child pornography, many consumers of child pornography have been found to download, view, and then delete child pornography on their digital devices on a cyclical and repetitive basis.

38. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[8]

39. Consumers of child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, e-mail, bulletin boards, chat sites, web forums, instant messaging

---

[7] *See United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections).

[8] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

applications, and other similar vehicles of communication.

40. Consumers of child pornography often collect, read, copy, or maintain names, screen names or nicknames, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in written hardcopy, on computer storage devices, or merely on scraps of paper.

41. Based upon my training and experience, I know that persons engaged in the production and possession of child erotica are also often involved in the production and possession of child pornography. Likewise, I know from training and experience that persons involved in the production and possession of child pornography are often involved in the production and possession of child erotica.

42. Based on my training, knowledge, experience, and conversations with others in law enforcement, I understand that an individual who possesses images and/or videos depicting child pornography on one digital storage device and/or Internet email or online storage account is likely to possess child pornography on additional digital storage devices and/or Internet email or online storage accounts that he possesses or controls. Additionally, based on this training and experience, I understand that even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

43. Based on the facts outlined herein, I believe that the user of Freenet residing at the SUBJECT PREMISES likely displays characteristics common to consumers of child pornography. For example, a user at the SUBJECT PREMISES downloaded and installed the Freenet software on his computer, and requested blocks associated for three known child exploitation files which would have required him to ascertain the specific keys associated with those files over the course of multiple days.

Background on Child Pornography, Computers, and the Internet

44. I have had both training and experience in the investigation of computer-related crimes, including those involving child pornography. Based on my training, experience, and consultation with other law enforcement, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types

– to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital

information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Specifics of Search and Seizure of Computer Systems

45. As described above and in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

46. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the

storage medium until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

47. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic

evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence

or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping"

program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, pieces, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the

criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

48. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence—storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements—analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software

available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

49. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

50. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B. If, however, the law

enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

CONCLUSION

51. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

Sgt M. Sull

Task Force Officer Michael Sullivan
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____
(specify reliable electronic means)

Date	*Judge's signature*
City and State	*Magistrate Judge Lincoln D. Almond*

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at 284 S. Christopher Avenue in Tiverton, Rhode Island, including the residential building, any outbuildings, and any appurtenances thereto (the SUBJECT PREMISES). The SUBJECT PREMISES appears to be a tan, two story single family, with a red front door and two attached garages. To the left of the front door "284" is affixed.

ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 2252A (possession and receipt of child pornography), including:

A. The following topics:

1. Child pornography;

2. The sexual abuse or exploitation of children;

3. Child erotica;

4. The identity of any child depicted in videos and photographs located in the equipment or discussed in any communications related to child pornography or the sexual abuse or exploitation of children;

5. Internet activity reflecting a sexual interest in minors or child pornography;

6. Freenet;

7. Membership in online groups, clubs, or services that provide, make accessible, or otherwise concern child pornography.

B. Any communication(s) relating to child pornography, the sexual abuse or exploitation of children, or the identity of any child depicted in videos and photographs located in the equipment;

C. Any social media account(s) or communication application(s) used to send or receive any communication(s) relating to child pornography, the sexual abuse or exploitation of children, or the identity of any child depicted in videos and photographs located in the equipment;

D. The identity, location, and travel of any co-conspirators, as well as any co-

conspirators' acts taken in furtherance of the crimes listed above;

E. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter forensic programs and associated data that are designed to eliminate data;

5. evidence indicating how and when the computer equipment was accessed or used;

6. records of or information about any Internet Protocol addresses used;

7. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

8. records and tangible objects pertaining to accounts held with companies providing internet access or remote storage of either data or storage media;

9. records of or information about the computer equipment's internet activity; and

10. contextual information necessary to understand the evidence described in this attachment.

F. Records and tangible objects relating to the ownership, occupancy, or use of the SUBJECT PREMISES (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers); and

G. Records, information, and items relating to the ownership or use of computer equipment found in the SUBJECT PREMISES or on the person of the Subject, including sales receipts, bills for Internet access, and handwritten notes.

II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in Paragraph I.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. A "record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

H. "Child Pornography," as defined in 18 U.S.C. § 2256(8)(A), means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

I. "Child Erotica" means materials or items that are sexually arousing to persons

having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.

EXECUTION

Searching agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence authorized by this warrant, as outlined above. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If the computer equipment contains contraband, it will not be returned. If the computer equipment cannot be returned, agents will attempt to make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do

not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.